# TEL2813/IS2820
# Security Management

Risk Management:
Identifying and Assessing Risk
Lecture 7
Feb 17, 2005

## Introduction

- Information security departments are created primarily to manage IT risk
- Managing risk is one of the key responsibilities of every manager within the organization
- In any well-developed risk management program, two formal processes are at work:
  - Risk identification and assessment
  - Risk control

## Knowing Our Environment

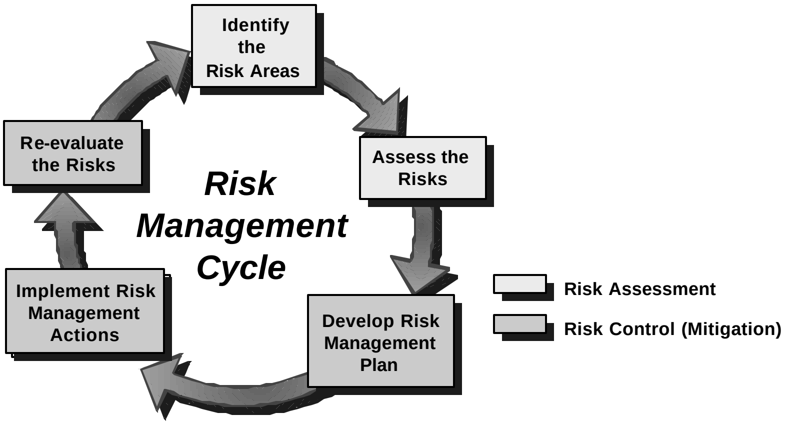
- Identify, Examine and Understand
  - information and how it is processed, stored, and transmitted
- Initiate an in-depth risk management program
- Risk management is a process
  - means - safeguards and controls that are devised and implemented are not install-and-forget devices

## Knowing the Enemy

- Identify, examine, and understand
  - *the threats*
- Managers must be prepared
  - to fully identify those threats that pose risks to the organization and the security of its information assets
- Risk management is the process
  - of assessing the risks to an organization's information and determining how those risks can be controlled or mitigated

# Risk Management

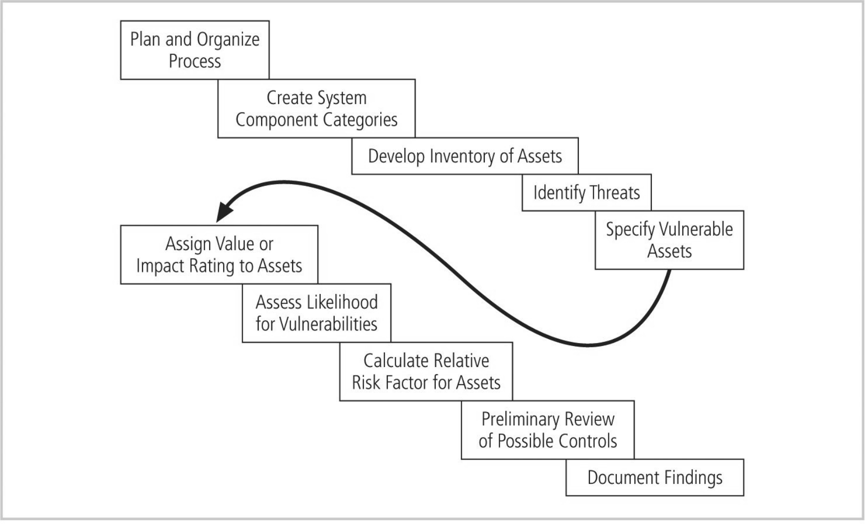
- The process concerned with identification, measurement, control and minimization of security risks in information systems to a level commensurate with the value of the assets protected (NIST)



# Accountability for Risk Management

- All communities of interest must work together:
  - Evaluating risk controls
  - Determining which control options are cost-effective
  - Acquiring or installing appropriate controls
  - Overseeing processes to ensure that controls remain effective
  - Identifying risks
  - Assessing risks
  - Summarizing findings

# Risk Identification Process



Plan and Organize Process

Create System Component Categories

Develop Inventory of Assets

Identify Threats

Specify Vulnerable Assets

Assign Value or Impact Rating to Assets

Assess Likelihood for Vulnerabilities

Calculate Relative Risk Factor for Assets

Preliminary Review of Possible Controls

Document Findings

**FIGURE 7-1** Risk Identification Process

# Risk Identification

- Risk identification
  - begins with the process of self-examination
- Managers
  - identify the organization’s information assets,
  - classify them into useful groups, and
  - prioritize them by their overall importance

## Creating an Inventory of Information Assets

- Identify information assets, including
  - people, procedures, data and information, software, hardware, and networking elements
- Should be done without pre-judging value of each asset
  - Values will be assigned later in the process

## Organizational Assets

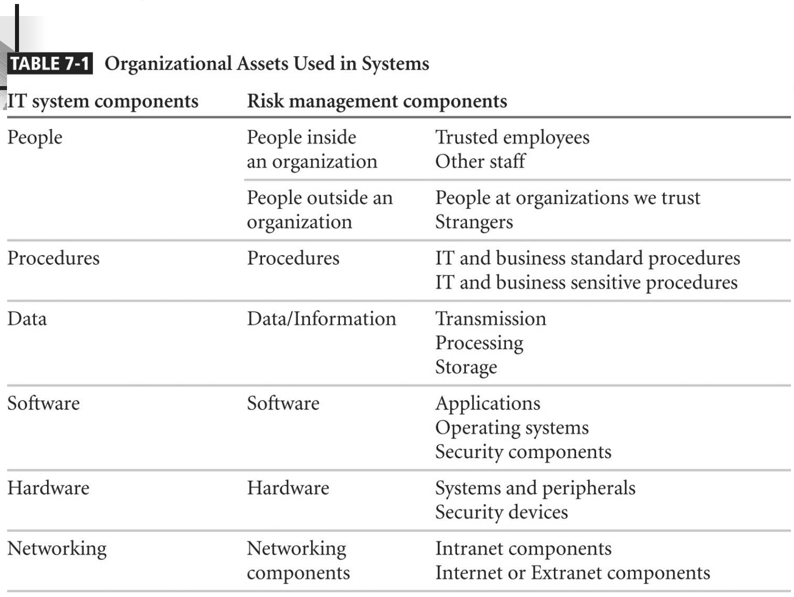


**TABLE 7-1** Organizational Assets Used in Systems

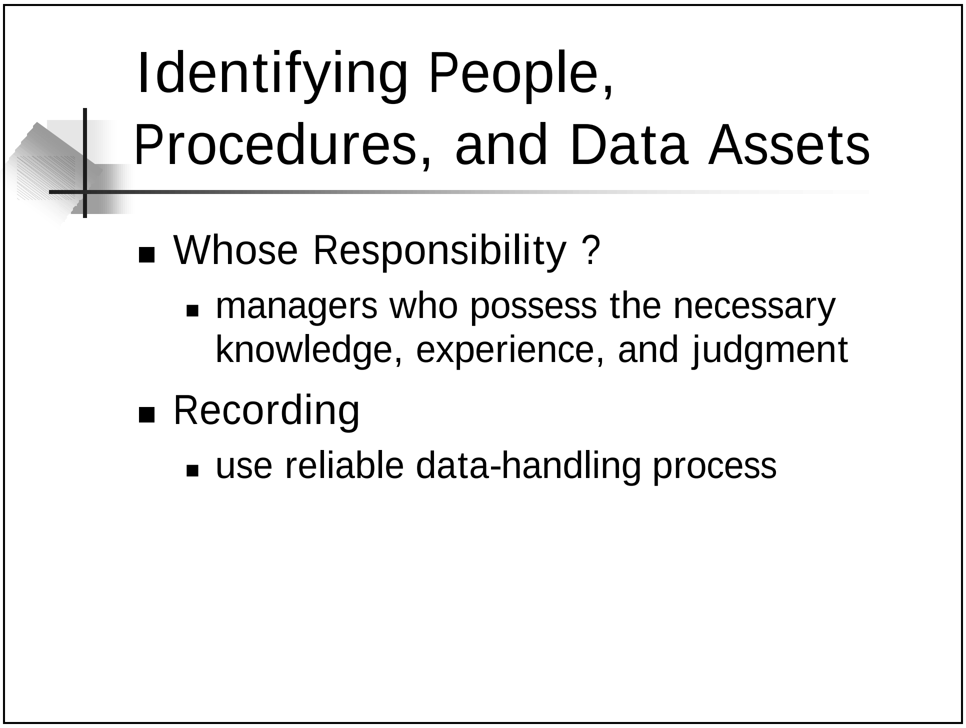
| IT system components | Risk management components | |
|---|---|---|
| People | People inside an organization | Trusted employees<br>Other staff |
| | People outside an organization | People at organizations we trust<br>Strangers |
| Procedures | Procedures | IT and business standard procedures<br>IT and business sensitive procedures |
| Data | Data/Information | Transmission<br>Processing<br>Storage |
| Software | Software | Applications<br>Operating systems<br>Security components |
| Hardware | Hardware | Systems and peripherals<br>Security devices |
| Networking | Networking components | Intranet components<br>Internet or Extranet components |

## Identifying Hardware, Software, and Network Assets

- Inventory process requires a certain amount of planning
- Determine which attributes of each of these information assets should be tracked
  - Will depend on the needs of the organization and
  - its risk management efforts

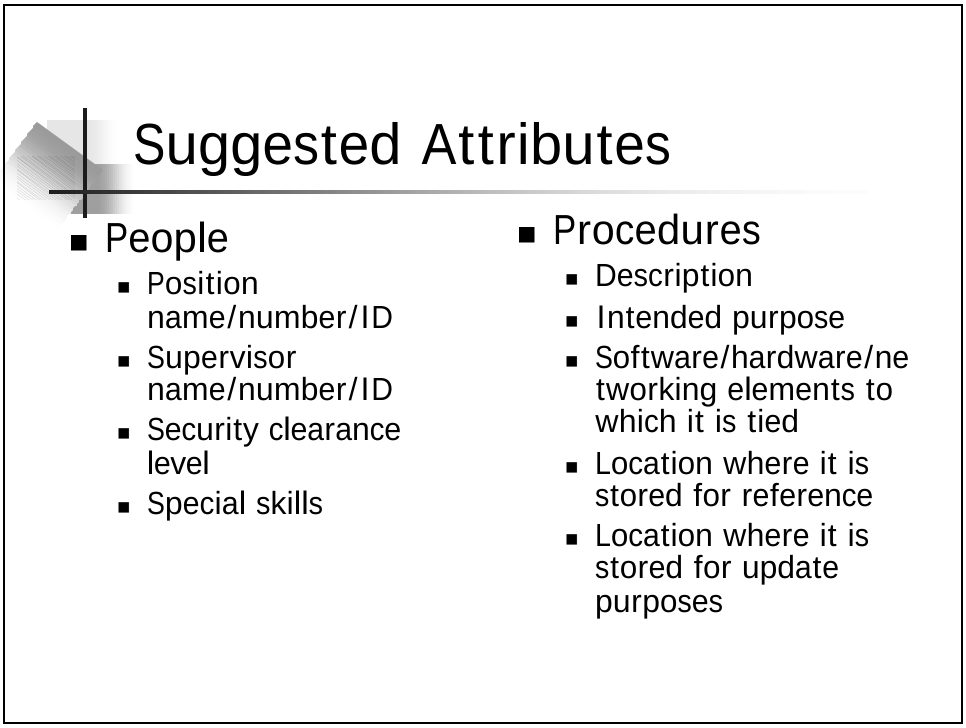
## Attributes for Assets

- Potential attributes:
  - Name
  - IP address
  - MAC address
  - Asset type
  - Manufacturer name
  - Manufacturer’s model or part number
    - Software version, update revision,
  - Physical location
  - Logical location
  - Controlling entity



## Identifying People, Procedures, and Data Assets

- Whose Responsibility ?
  - managers who possess the necessary knowledge, experience, and judgment
- Recording
  - use reliable data-handling process



## Suggested Attributes

- People
  - Position name/number/ID
  - Supervisor name/number/ID
  - Security clearance level
  - Special skills

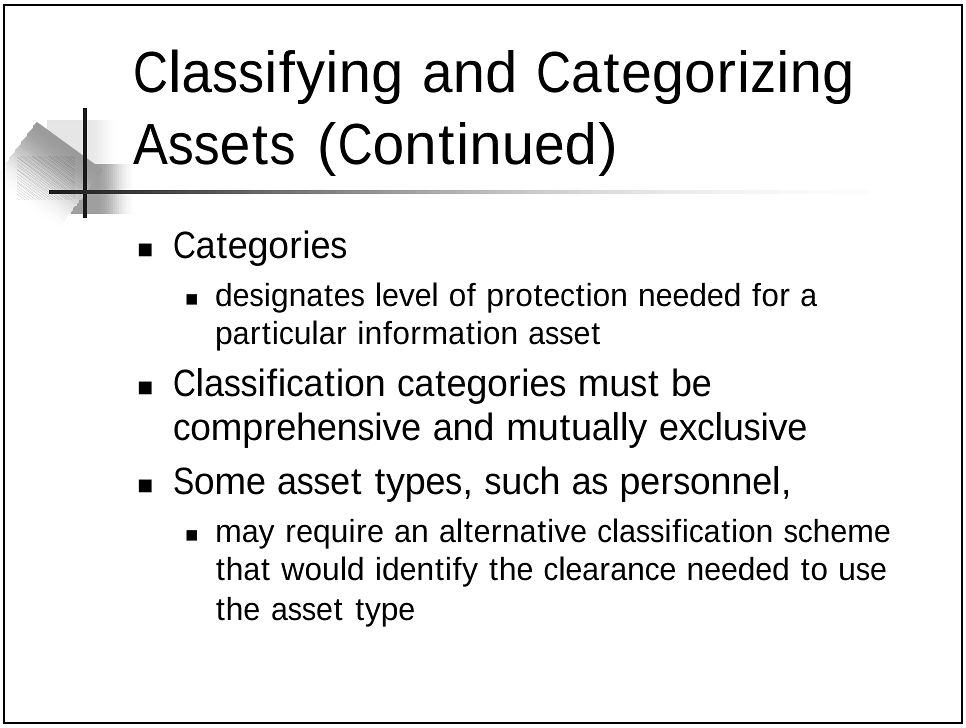
- Procedures
  - Description
  - Intended purpose
  - Software/hardware/networking elements to which it is tied
  - Location where it is stored for reference
  - Location where it is stored for update purposes

## Suggested Attributes

- Data
  - Classification
  - Owner/creator/manager
  - Size of data structure
  - Data structure used
  - Online or offline
  - Location
  - Backup procedures

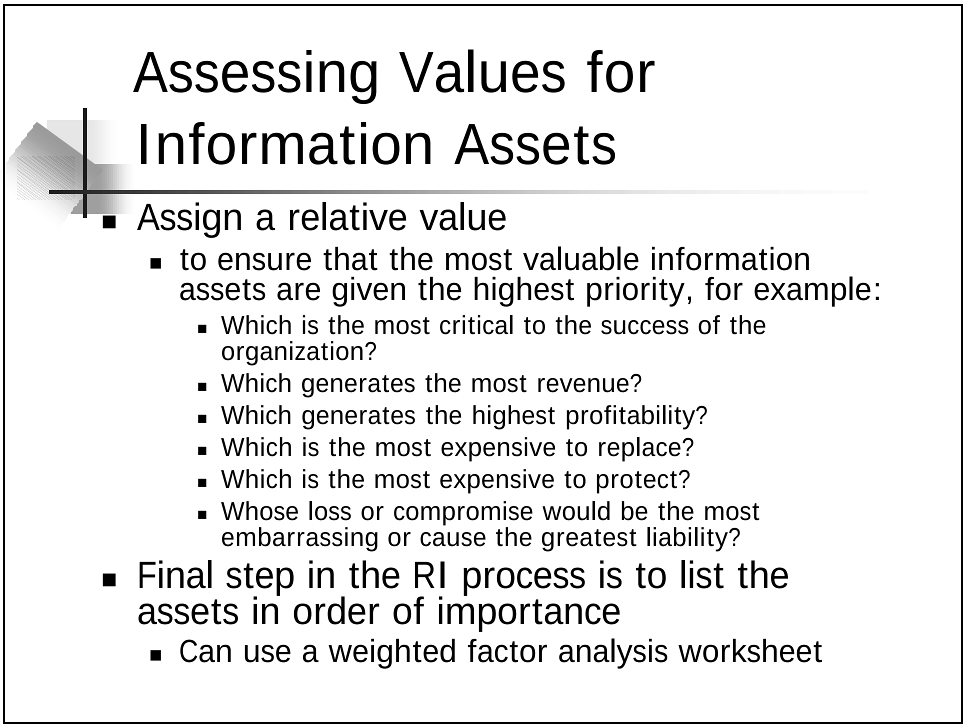
## Classifying and Categorizing Assets

- Determine whether its asset categories are meaningful
  - After initial inventory is assembled,
- Inventory should also reflect sensitivity and security priority assigned to each asset
- A classification scheme categorizes these information assets based on their sensitivity and security needs



# Classifying and Categorizing Assets (Continued)

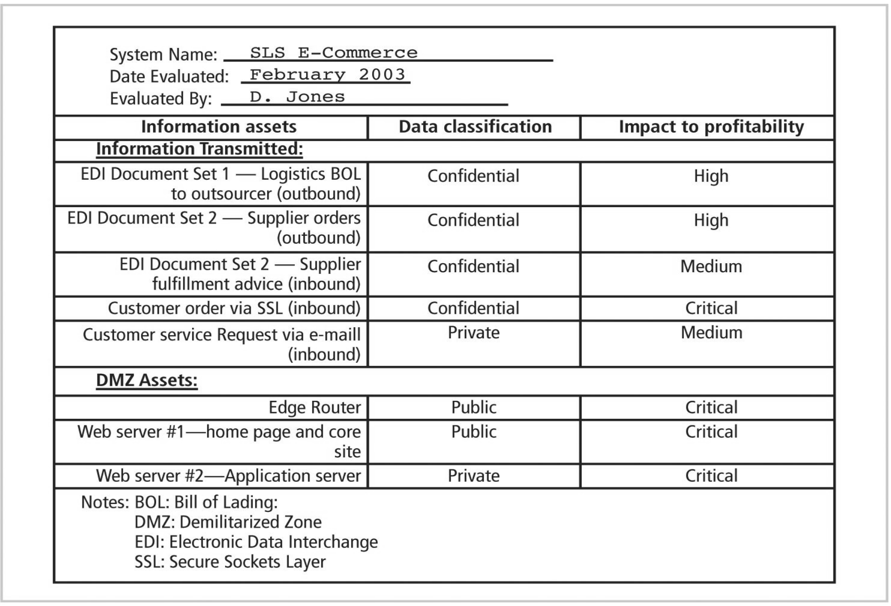
- Categories
  - designates level of protection needed for a particular information asset
- Classification categories must be comprehensive and mutually exclusive
- Some asset types, such as personnel,
  - may require an alternative classification scheme that would identify the clearance needed to use the asset type



# Assessing Values for Information Assets

- Assign a relative value
  - to ensure that the most valuable information assets are given the highest priority, for example:
    - Which is the most critical to the success of the organization?
    - Which generates the most revenue?
    - Which generates the highest profitability?
    - Which is the most expensive to replace?
    - Which is the most expensive to protect?
    - Whose loss or compromise would be the most embarrassing or cause the greatest liability?
- Final step in the RI process is to list the assets in order of importance
  - Can use a weighted factor analysis worksheet

## Sample Asset Classification Worksheet



System Name: SLS E-Commerce
Date Evaluated: February 2003
Evaluated By: D. Jones

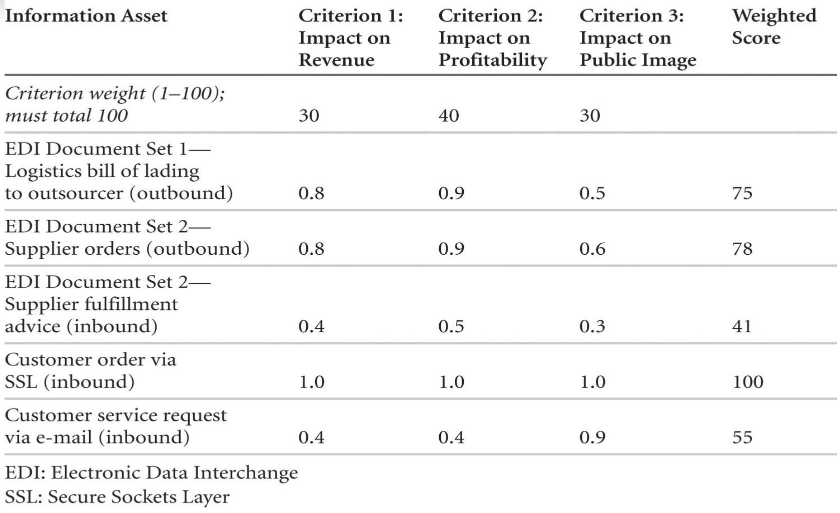
| Information assets | Data classification | Impact to profitability |
|---|---|---|
| **Information Transmitted:** | | |
| EDI Document Set 1 — Logistics BOL to outsourcer (outbound) | Confidential | High |
| EDI Document Set 2 — Supplier orders (outbound) | Confidential | High |
| EDI Document Set 2 — Supplier fulfillment advice (inbound) | Confidential | Medium |
| Customer order via SSL (inbound) | Confidential | Critical |
| Customer service Request via e-maill (inbound) | Private | Medium |
| **DMZ Assets:** | | |
| Edge Router | Public | Critical |
| Web server #1—home page and core site | Public | Critical |
| Web server #2—Application server | Private | Critical |

Notes: BOL: Bill of Lading:
DMZ: Demilitarized Zone
EDI: Electronic Data Interchange
SSL: Secure Sockets Layer

**FIGURE 7-2** Sample Asset Classification Worksheet

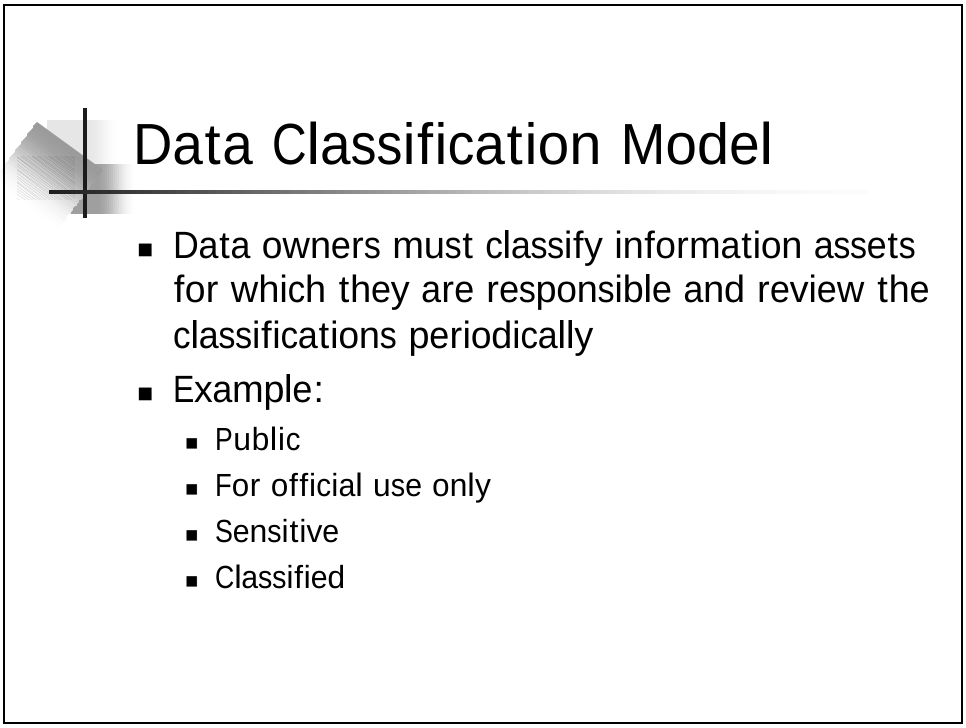
## Weighted Factor Analysis Worksheet (NIST SP 800-30)

**TABLE 7-2** Example Weighted Factor Analysis Worksheet



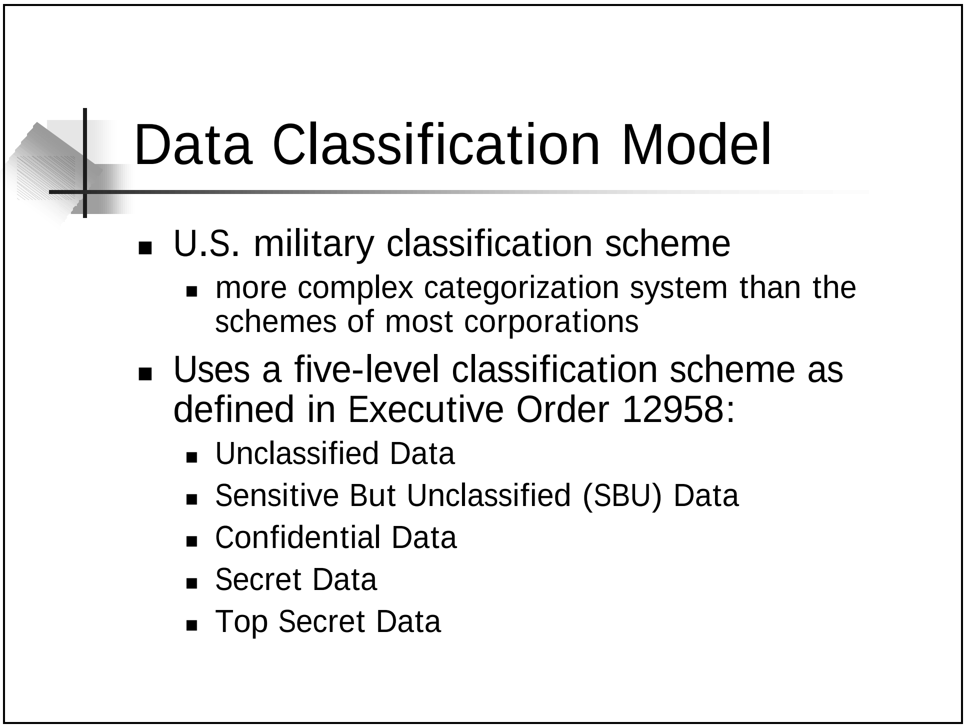
| Information Asset | Criterion 1: Impact on Revenue | Criterion 2: Impact on Profitability | Criterion 3: Impact on Public Image | Weighted Score |
|---|---|---|---|---|
| *Criterion weight (1–100); must total 100* | 30 | 40 | 30 | |
| EDI Document Set 1—Logistics bill of lading to outsourcer (outbound) | 0.8 | 0.9 | 0.5 | 75 |
| EDI Document Set 2—Supplier orders (outbound) | 0.8 | 0.9 | 0.6 | 78 |
| EDI Document Set 2—Supplier fulfillment advice (inbound) | 0.4 | 0.5 | 0.3 | 41 |
| Customer order via SSL (inbound) | 1.0 | 1.0 | 1.0 | 100 |
| Customer service request via e-mail (inbound) | 0.4 | 0.4 | 0.9 | 55 |

EDI: Electronic Data Interchange
SSL: Secure Sockets Layer



## Data Classification Model

- Data owners must classify information assets for which they are responsible and review the classifications periodically
- Example:
  - Public
  - For official use only
  - Sensitive
  - Classified



## Data Classification Model

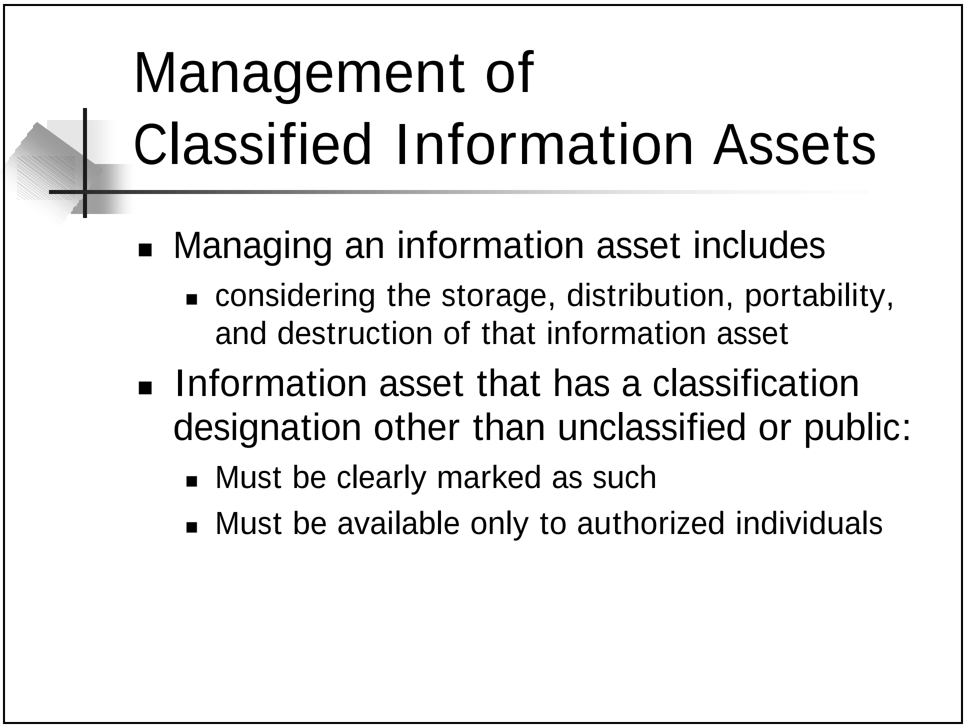
- U.S. military classification scheme
  - more complex categorization system than the schemes of most corporations
- Uses a five-level classification scheme as defined in Executive Order 12958:
  - Unclassified Data
  - Sensitive But Unclassified (SBU) Data
  - Confidential Data
  - Secret Data
  - Top Secret Data

# Security Clearances

- Personnel Security Clearance Structure:
  - Complement to data classification scheme
  - Each user of information asset is assigned an authorization level that indicates level of information classification he or she can access
- Most organizations have developed a set of roles and corresponding security clearances
  - Individuals are assigned into groups that correlate with classifications of the information assets they need for their work

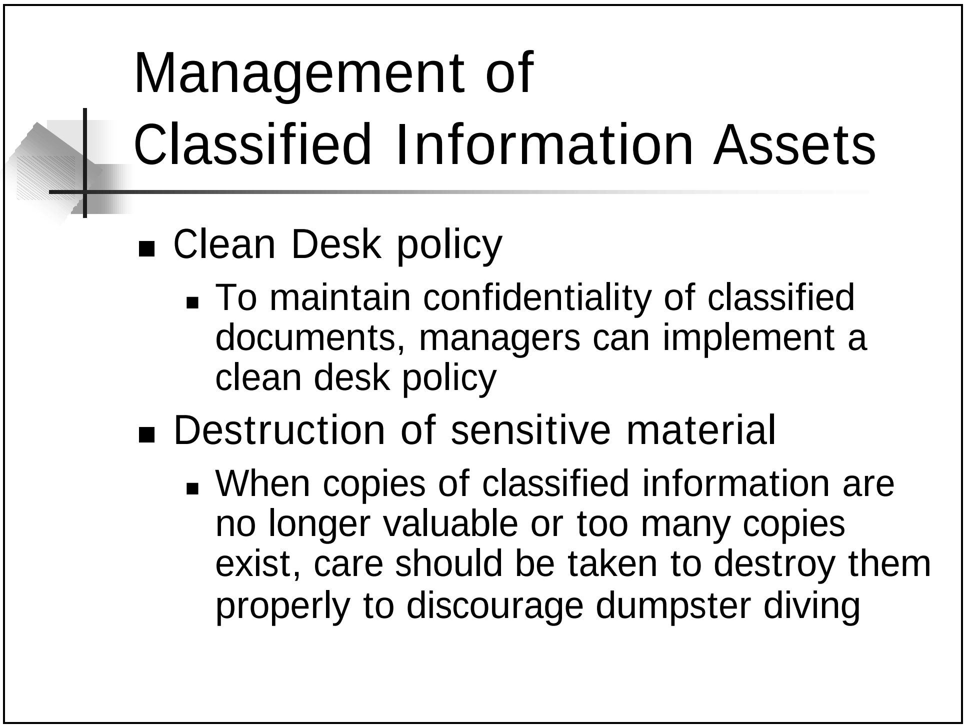
# Security Clearances (Continued)

- Need-to-know principle:
  - Regardless of one’s security clearance, an individual is not allowed to view data simply because it falls within that individual’s level of clearance
  - Before he or she is allowed access to a specific set of data, that person must also need-to-know the data as well



## Management of Classified Information Assets

- Managing an information asset includes
  - considering the storage, distribution, portability, and destruction of that information asset
- Information asset that has a classification designation other than unclassified or public:
  - Must be clearly marked as such
  - Must be available only to authorized individuals



## Management of Classified Information Assets

- Clean Desk policy
  - To maintain confidentiality of classified documents, managers can implement a clean desk policy
- Destruction of sensitive material
  - When copies of classified information are no longer valuable or too many copies exist, care should be taken to destroy them properly to discourage dumpster diving

# Threat Identification

- Any organization typically faces a wide variety of threats
- If you assume that every threat can and will attack every information asset, then the project scope becomes too complex
- To make the process less unwieldy, manage separately
  - each step in the threat identification and
  - vulnerability identification processes

  then coordinate them at the end

# Identify And Prioritize Threats and Threat Agents

- Each threat presents a unique challenge to information security
  - Must be handled with specific controls that directly address particular threat and threat agent's attack strategy
- Threat assessment
  - Before threats can be assessed in risk identification process, each threat must be further examined to determine its potential to affect targeted information asset

# Threats to Information Security

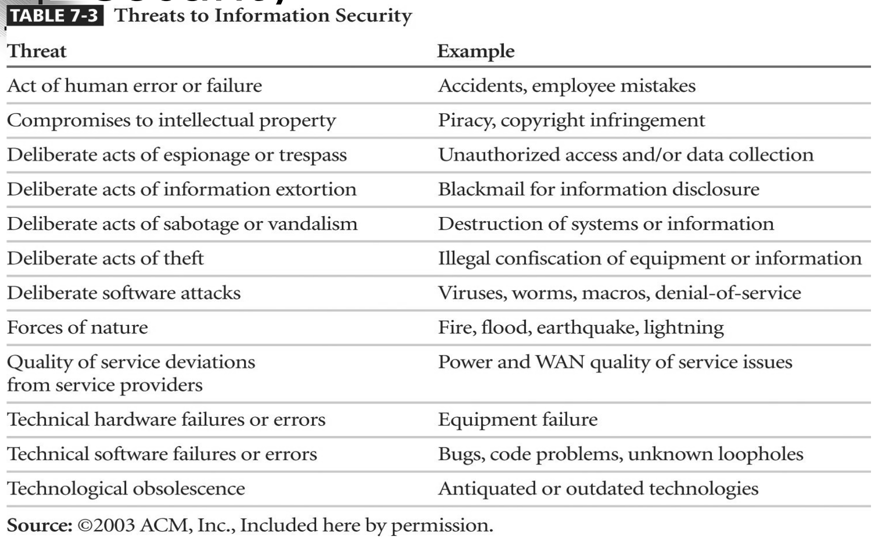
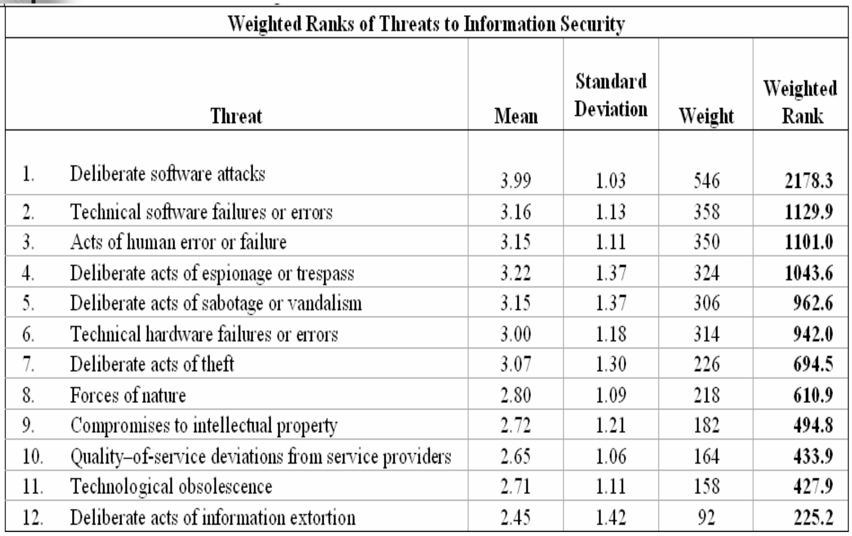


TABLE 7-3 Threats to Information Security

| Threat | Example |
|---|---|
| Act of human error or failure | Accidents, employee mistakes |
| Compromises to intellectual property | Piracy, copyright infringement |
| Deliberate acts of espionage or trespass | Unauthorized access and/or data collection |
| Deliberate acts of information extortion | Blackmail for information disclosure |
| Deliberate acts of sabotage or vandalism | Destruction of systems or information |
| Deliberate acts of theft | Illegal confiscation of equipment or information |
| Deliberate software attacks | Viruses, worms, macros, denial-of-service |
| Forces of nature | Fire, flood, earthquake, lightning |
| Quality of service deviations from service providers | Power and WAN quality of service issues |
| Technical hardware failures or errors | Equipment failure |
| Technical software failures or errors | Bugs, code problems, unknown loopholes |
| Technological obsolescence | Antiquated or outdated technologies |

**Source:** ©2003 ACM, Inc., Included here by permission.

# Threats to Information Security



Weighted Ranks of Threats to Information Security

| Threat | Mean | Standard Deviation | Weight | Weighted Rank |
|---|---|---|---|---|
| 1. Deliberate software attacks | 3.99 | 1.03 | 546 | **2178.3** |
| 2. Technical software failures or errors | 3.16 | 1.13 | 358 | **1129.9** |
| 3. Acts of human error or failure | 3.15 | 1.11 | 350 | **1101.0** |
| 4. Deliberate acts of espionage or trespass | 3.22 | 1.37 | 324 | **1043.6** |
| 5. Deliberate acts of sabotage or vandalism | 3.15 | 1.37 | 306 | **962.6** |
| 6. Technical hardware failures or errors | 3.00 | 1.18 | 314 | **942.0** |
| 7. Deliberate acts of theft | 3.07 | 1.30 | 226 | **694.5** |
| 8. Forces of nature | 2.80 | 1.09 | 218 | **610.9** |
| 9. Compromises to intellectual property | 2.72 | 1.21 | 182 | **494.8** |
| 10. Quality–of-service deviations from service providers | 2.65 | 1.06 | 164 | **433.9** |
| 11. Technological obsolescence | 2.71 | 1.11 | 158 | **427.9** |
| 12. Deliberate acts of information extortion | 2.45 | 1.42 | 92 | **225.2** |

# Weighted Ranking of Threat-Driven Expenditures

| Top Threat-Driven Expenses | Rating |
|---|---|
| Deliberate software attacks | 12.7 |
| Acts of human error or failure | 7.6 |
| Technical software failures or errors | 7.0 |
| Technical hardware failures or errors | 6.0 |
| QoS deviations from service providers | 4.9 |
| Deliberate acts of espionage or trespass | 4.7 |
| Deliberate acts of theft | 4.1 |
| Deliberate acts of sabotage or vandalism | 4.0 |
| Technological obsolescence | 3.3 |
| Forces of nature | 3.0 |
| Compromises to intellectual property | 2.2 |
| Deliberate acts of information extortion | 1.0 |

# Vulnerability Assessment

- Steps revisited
  - Identify the information assets of the organization and
  - Document some threat assessment criteria,
  - Begin to review every information asset for each threat
    - Leads to creation of list of vulnerabilities that remain potential risks to organization
- Vulnerabilities
  - specific avenues that threat agents can exploit to attack an information asset
- At the end of the risk identification process,
  - a list of assets and their vulnerabilities has been developed

## Introduction to Risk Assessment

- The goal at this point is to create a method to evaluate relative risk of each listed vulnerability

## Risk Identification Estimate Factors

**Risk** is

The likelihood of the occurrence of a vulnerability

*Multiplied by*

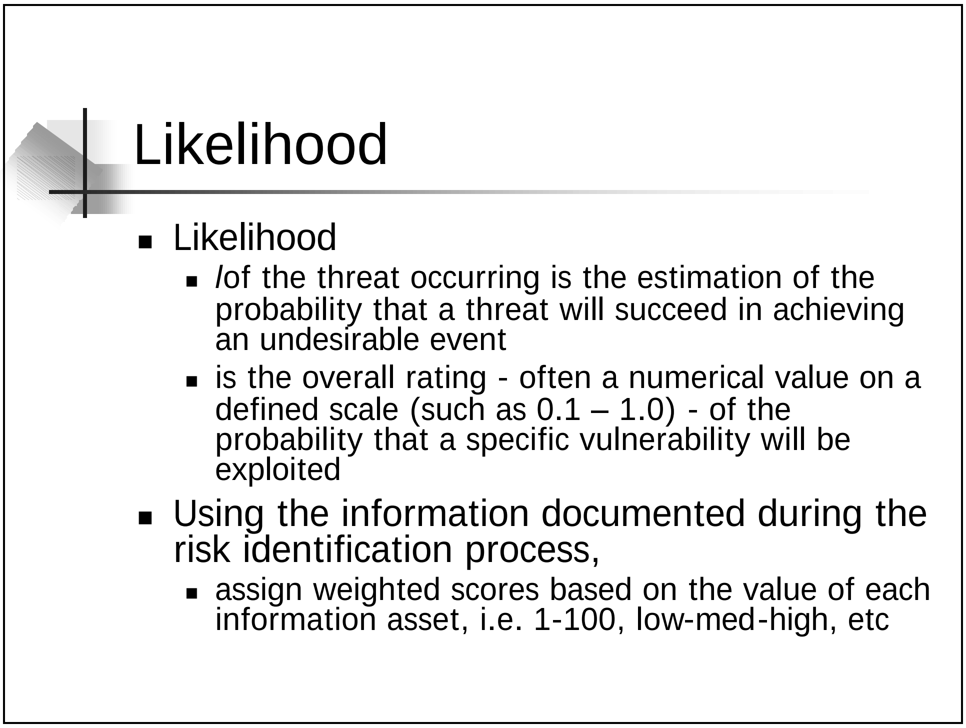
The value of the information asset

*Minus*

The percentage of risk mitigated by current controls

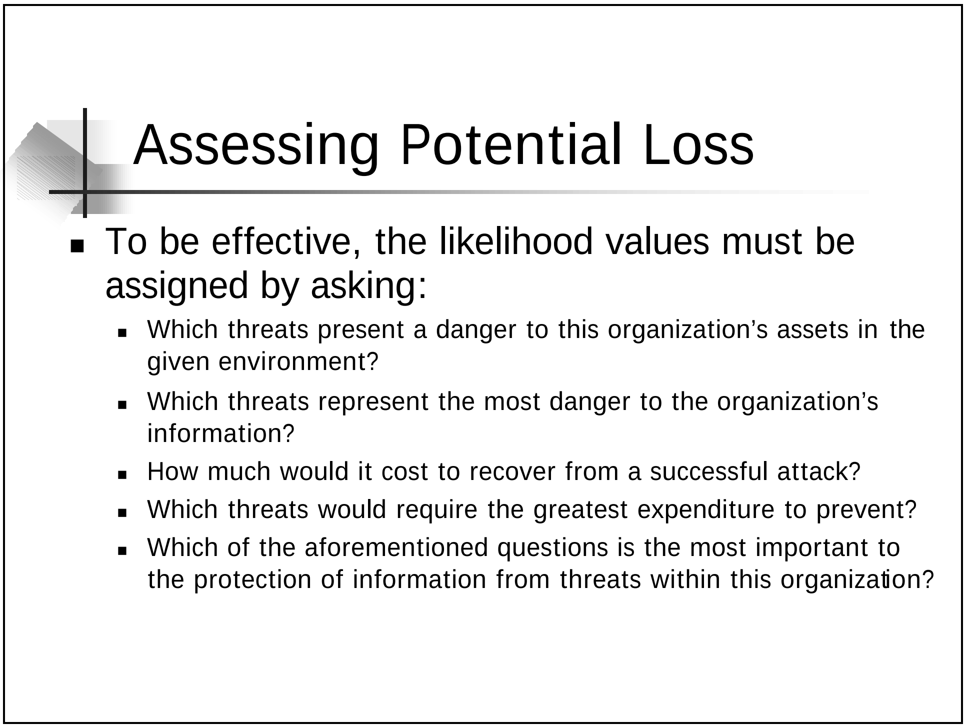
*Plus*

The uncertainty of current knowledge of the vulnerability



# Likelihood

- Likelihood
  - /of the threat occurring is the estimation of the probability that a threat will succeed in achieving an undesirable event
  - is the overall rating - often a numerical value on a defined scale (such as 0.1 – 1.0) - of the probability that a specific vulnerability will be exploited
- Using the information documented during the risk identification process,
  - assign weighted scores based on the value of each information asset, i.e. 1-100, low-med-high, etc



# Assessing Potential Loss

- To be effective, the likelihood values must be assigned by asking:
  - Which threats present a danger to this organization’s assets in the given environment?
  - Which threats represent the most danger to the organization’s information?
  - How much would it cost to recover from a successful attack?
  - Which threats would require the greatest expenditure to prevent?
  - Which of the aforementioned questions is the most important to the protection of information from threats within this organization?

# Mitigated Risk / Uncertainty

- If it is partially controlled,
  - Estimate what percentage of the vulnerability has been controlled
- Uncertainty
  - is an estimate made by the manager using judgment and experience
  - It is not possible to know everything about every vulnerability
  - The degree to which a current control can reduce risk is also subject to estimation error

# Risk Determination Example

- Asset A has a value of 50 and has vulnerability #1,
  - likelihood of 1.0 with no current controls
  - assumptions and data are 90% accurate
- Asset B has a value of 100 and has two vulnerabilities
  - Vulnerability #2
    - likelihood of 0.5 with a current control that addresses 50% of its risk
  - Vulnerability # 3
    - likelihood of 0.1 with no current controls
    - assumptions and data are 80% accurate

## Risk Determination Example

- Resulting ranked list of risk ratings for the three vulnerabilities is as follows:
  - Asset A: Vulnerability 1 rated as 55 =
    - (50 × 1.0) – 0% + 10%
  - Asset B: Vulnerability 2 rated as 35 =
    - (100 × 0.5) – 50% + 20%
  - Asset B: Vulnerability 3 rated as 12 =
    - (100 × 0.1) – 0 % + 20%

## Identify Possible Controls

- For each threat and its associated vulnerabilities that have residual risk, create a preliminary list of control ideas
- Three general categories of controls exist:
  - Policies
  - Programs
  - Technical controls

## Access Controls

- Access controls specifically
  - address admission of a user into a trusted area of the organization
- These areas can include
  - information systems,
  - physically restricted areas such as computer rooms, and
  - even the organization in its entirety
- Access controls usually consist of
  - a combination of policies, programs, and technologies

## Types of Access Controls

- Mandatory Access Controls (MACs):
  - Required
  - Structured and coordinated with a data classification scheme
  - When implemented, users and data owners have limited control over their access to information resources
  - Use data classification scheme that rates each collection of information

# Types of Access Controls (Continued)

- Access Control Matrix
- Access Control List
  - the column of attributes associated with a particular object is called an access control list (ACL)
- Capabilities
  - The row of attributes associated with a particular subject

# Types of Access Controls (Continued)

- Nondiscretionary controls are determined by a central authority in the organization
  - Can be based on roles—called role-based controls—or on a specified set of tasks—called task-based controls
  - Task-based controls can, in turn, be based on lists maintained on subjects or objects
  - Role-based controls are tied to the role that a particular user performs in an organization, whereas task-based controls are tied to a particular assignment or responsibility

# Types of Access Controls (Continued)

- Discretionary Access Controls (DACs) are
  - implemented at the discretion or option of the data user
- The ability to share resources in a peer-to-peer configuration allows
  - users to control and possibly provide access to information or resources at their disposal
- The users can allow
  - general, unrestricted access, or
  - specific individuals or sets of individuals to access these resources

# Documenting the Results of Risk Assessment

- The goal of the risk management process:
  - Identify information assets and their vulnerabilities
  - Rank them according to the need for protection
- In preparing this list, collect
  - wealth of factual information about the assets and the threats they face
  - information about the controls that are already in place
- The final summarized document is the ranked vulnerability risk worksheet

## Ranked Vulnerability Risk Worksheet

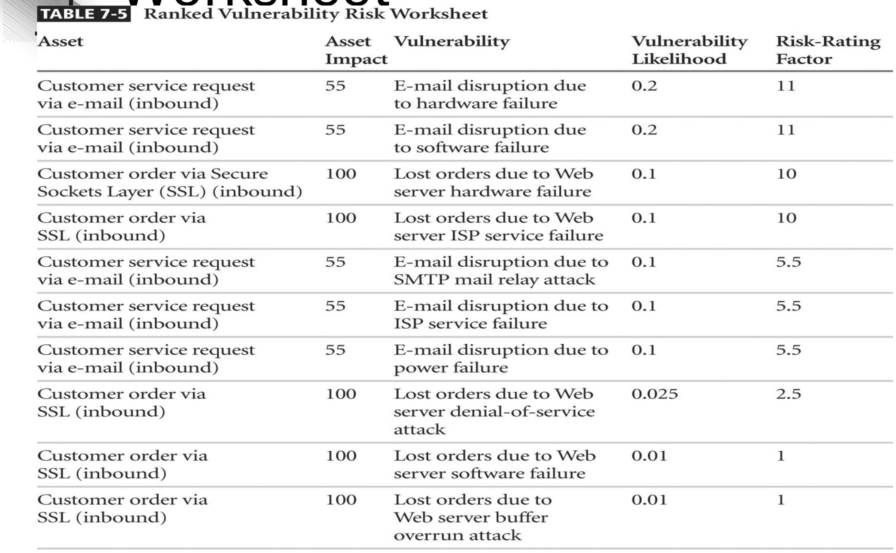


TABLE 7-5 Ranked Vulnerability Risk Worksheet

| Asset | Asset Impact | Vulnerability | Vulnerability Likelihood | Risk-Rating Factor |
|---|---|---|---|---|
| Customer service request via e-mail (inbound) | 55 | E-mail disruption due to hardware failure | 0.2 | 11 |
| Customer service request via e-mail (inbound) | 55 | E-mail disruption due to software failure | 0.2 | 11 |
| Customer order via Secure Sockets Layer (SSL) (inbound) | 100 | Lost orders due to Web server hardware failure | 0.1 | 10 |
| Customer order via SSL (inbound) | 100 | Lost orders due to Web server ISP service failure | 0.1 | 10 |
| Customer service request via e-mail (inbound) | 55 | E-mail disruption due to SMTP mail relay attack | 0.1 | 5.5 |
| Customer service request via e-mail (inbound) | 55 | E-mail disruption due to ISP service failure | 0.1 | 5.5 |
| Customer service request via e-mail (inbound) | 55 | E-mail disruption due to power failure | 0.1 | 5.5 |
| Customer order via SSL (inbound) | 100 | Lost orders due to Web server denial-of-service attack | 0.025 | 2.5 |
| Customer order via SSL (inbound) | 100 | Lost orders due to Web server software failure | 0.01 | 1 |
| Customer order via SSL (inbound) | 100 | Lost orders due to Web server buffer overrun attack | 0.01 | 1 |

## Documenting the Results of Risk Assessment (Continued)

- What are the deliverables from this stage of the risk management project?
- The risk identification process should designate
  - what function the reports serve,
  - who is responsible for preparing them, and
  - who reviews them

# Risk Identification and Assessment Deliverables

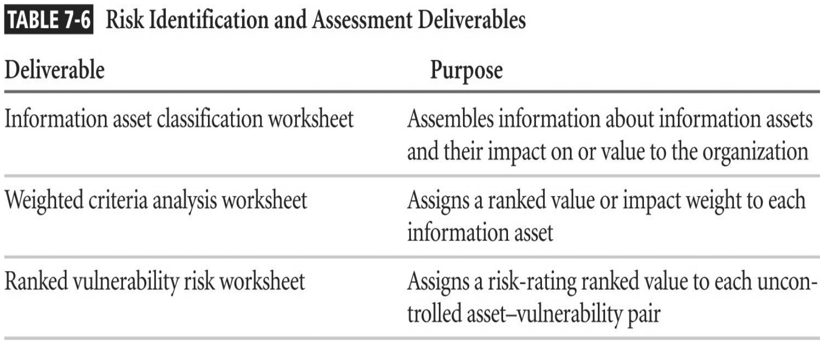


**TABLE 7-6** Risk Identification and Assessment Deliverables

| Deliverable | Purpose |
|---|---|
| Information asset classification worksheet | Assembles information about information assets and their impact on or value to the organization |
| Weighted criteria analysis worksheet | Assigns a ranked value or impact weight to each information asset |
| Ranked vulnerability risk worksheet | Assigns a risk-rating ranked value to each uncontrolled asset–vulnerability pair |